Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554



| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Communications Assistance for Law Enforcement Act | ) | CC Docket No. 97-213 |
| | ) | |

# REPLY COMMENTS OF U S WEST, INC.

Of Counsel,

Dan L. Poole
U S WEST, Inc.

William T. Lake
John H. Harwood II
Samir Jain
Todd Zubler
Wilmer, Cutler & Pickering
2445 M Street, N.W.
Washington, DC 20037
(202) 663-6000

Kathryn Marie Krause
Edward M. Chavez
Suite 700
1020 19th Street, N.W.
Washington, DC 20036
(303) 672-2859

Attorneys for

U S WEST, INC.

February 11, 1998

TABLE OF CONTENTS

Page

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Communications Assistance for Law Enforcement Act | ) | CC Docket No. 97-213 |
| | ) | |

# REPLY COMMENTS OF U S WEST, INC.

## I. INTRODUCTION AND SUMMARY

It is clear from the opening comments in this proceeding that the Federal Communications Commission ("Commission") should adopt a far less regulatory approach to implementing the requirements of the Communications Assistance to Law Enforcement Act ("CALEA") than that set out in the Notice of Proposed Rulemaking.[1] The Notice's proposals for regulating carriers, combined with CALEA's looming compliance deadlines, create difficult -- generally insurmountable -- burdens for carriers, without advancing the statute's objectives in the least. The Commission should ensure that any regulations imposed at the conclusion of this proceeding go no further than is demonstrably necessary to achieve those objectives.

First, the Commission should declare that all information services are exempt from CALEA's requirements regardless of what type of entity provides the services. U S WEST demonstrated in our comments why the statutory language

[1] In the Matter of: Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, Notice of Proposed Rulemaking, FCC 97-356, rel. Oct. 10, 1997 ("Notice" or "NPRM").

itself requires this outcome. Other commentors addressing this matter are unanimous in support of this position.[2]

Second, the Commission must reconsider whether the Notice's proposed regulations of carrier procedures are consistent with CALEA's purpose. Both the text and legislative history of the statute confirm that CALEA was directed at ensuring network interception capabilities and system security, not at regulating all carrier interception procedures. In promulgating rules under Section 229, the Commission should give considerable weight to carriers' excellent record on interception procedures and security.

Third, industry now has adopted a technical standard for CALEA capabilities. Under the statute, this standard constitutes a safe harbor, unless and until the Commission acts pursuant to an objection filed in accordance with Section 107. The FBI's discussion of CALEA capabilities in the instant proceeding is immaterial to the sufficiency of the existing industry standard. The Commission should take care not to prejudge the merits of any of these issues in the context of this proceeding.

Fourth, the comments reveal broad industry consensus that compliance with the capability requirements of CALEA is not reasonably achievable at this time and cannot be reasonably achievable until CALEA-compliant equipment is commercially

---

[2] The Federal Bureau of Investigation ("FBI"), while supporting the general proposition, proposes -- somewhat inscrutably given the statutory definitions in the Telecommunications Act of 1996 ("1996 Act" or "Act") -- a narrow definition of "information services." The FBI's position is discussed in more detail in Section II, below.

available on an industrywide basis. For this reason, U S WEST joins with those commentors that urge the Commission to grant a blanket two-year extension of the compliance date. Furthermore, the Commission should make clear that further extensions will be given if compliant equipment is not commercially available at the time of the extended deadline.

## II. ALL COMMENTORS AGREE THAT ALL INFORMATION SERVICES -- INCLUDING THOSE PROVIDED BY COMMON CARRIERS -- MUST BE EXCLUDED FROM SECTION 103 REQUIREMENTS

The comments reveal unanimous agreement that any information service provided by any entity is exempt from the requirements of CALEA.[3] Thus, the record in this proceeding confirms U S WEST's position that common carriers may provide information services without rendering them subject to Section 103.[4]

As U S WEST previously pointed out, the text of CALEA nowhere suggests that CALEA's exemption for information services applies only to entities providing exclusively such services. Indeed, Congress excluded information services from CALEA because call content has always been accorded greater protection than call identification.[5] It is irrelevant for that Congressional purpose whether an entity --

---

[3] The industry and public interest commentors (such as the American Civil Liberties Union, et al. ("ACLU") (at Section III) and the Center for Democracy and Technology ("CDT") (at 21-22)) expressly agree that information services provided by common carriers are exempt. And see AT&T Corp. ("AT&T") at 39-42; Cellular Telecommunications Industry Association ("CTIA") at 24-25. The FBI concurs, although its comments are somewhat elliptic on the subject. The FBI argues, for example, that a common carrier's transport access to information services should be subject to CALEA. See FBI at 14-15 ¶ 29. This argument implicitly recognizes that a common carrier's information services themselves are exempt from Section 103.

[4] See U S WEST Comments at 6-9.

[5] See ACLU at Section III.

such as a carrier -- provides information services on an exclusive basis or other services in addition to information services.

While acknowledging the statutory exclusion of information services, the FBI urges the Commission to adopt a "conservative" definition of the term "information services."[6] Whatever the FBI may mean by "conservative," it is clear from CALEA's text that "information services" must include those services known as "enhanced services" prior to the 1996 Act.

As noted in U S WEST's Comments, the Commission has already determined that the 1996 Act's definition of "information services" includes these "enhanced services."[7] CALEA's definition of "information services" is broader than the 1996 Act's definition.[8] Therefore, CALEA's category of "information services" must include all "information services" defined by the 1996 Act, including "enhanced services," and all "enhanced services" are accordingly exempt from the requirements of Section 103.

## III. THE COMMENTS DEMONSTRATE THAT THE NOTICE MISINTERPRETS THE PURPOSE OF CALEA'S CARRIER SECURITY REQUIREMENTS AND PROPOSES AN OVERLY INTRUSIVE REGULATORY STRUCTURE

In their comments, both industry and public interest groups make plain that the Notice's overall approach to carrier security is contrary to the letter and purpose of the statute. The Notice mistakenly assumes that Section 105 of CALEA aims to

---

[6] FBI at 14-15 ¶ 29.

[7] See U S WEST Comments at 10.

[8] See id. at 9-10.

prevent unlawful interceptions by carrier employees and that the Commission, therefore, has broad authority to regulate internal carrier personnel procedures.

### A. Section 105 Of CALEA Was Intended To Protect Against Remote Access To Switch Intelligence And To Ensure Carrier Participation In The Interception Process

CALEA's focus is on hardware/software (i.e., systems) capacity and capabilities, not internal carrier processes and procedures. As CDT persuasively demonstrates in its comments,[9] Congress enacted Section 105 of CALEA in response to the particular capabilities of new, switch-based interception technology, technology that more and more incorporates computer technology, thus -- at least theoretically -- becoming vulnerable to inappropriate access much like other computer technologies.

Section 105 requires a carrier to ensure that interceptions within its premises be activated only (1) "with a court order or other lawful authorization," and (2) "with the affirmative intervention of an individual officer or employee of the carrier."[10] As CDT notes in its comments,[11] CALEA's legislative history and other contemporaneous materials show that Section 105 was intended to address two related concerns arising from new, switch-based interception technologies: (1) that law enforcement might be able to access telephone switches remotely without carrier assistance,[12] and (2) that outside parties such as hackers might be able

---

[9] See CDT at 11-16. And see CTIA at 26.

[10] 47 U.S.C. § 1004.

[11] See CDT at 12; see also CTIA at 25-26.

implement unauthorized interceptions.[13]

Section 105 responds to these concerns quite precisely. Carriers are required to be affirmatively involved in all interceptions, and carriers must ensure that all interceptions are supported by a court order or other lawful authorization.

CALEA's legislative history, thus, does not support the expansive carrier practices/personnel requirements that the Notice proposes to place on carriers. There is no hint that Congress thought carrier personnel had suddenly become a security threat.[14] Indeed, given the already substantial incentives for carrier responsibility and the overall commendable record of carriers regarding interception security, it would have been remarkable for any congressperson or official to express such a concern.

The Notice's proposed burdensome requirements aimed at carrier practices and procedures therefore miss the point of the statutory concern. In place of the outlined proposals, the Commission should adopt a more flexible regulatory

---

[12] As numerous commentors confirm, CALEA was not directed at law enforcement's ability to implement interceptions in the local loop (that is, away from a carrier's switching premises). See, e.g., CDT at 9-11 and n.6; CTIA at 26 and n.43; FBI at 16 n.22.

[13] The House Report summarized the purpose of Section 105 as "mak[ing] clear that government agencies do not have the authority to activate remotely interceptions within the switching premises of a telecommunications carrier." H.R. Rep. No. 103-827, at 26 (1994), reprinted in 1995 U.S.C.C.A.N. 3489, 3506.

[14] Indeed, the legislative history's references to carrier personnel indicate that Congress desired their active involvement as a counterbalance to law enforcement. See id. at 18, reprinted in 1995 U.S.C.C.A.N. at 3498 (noting that statute "[r]equires affirmative intervention of common carriers' personnel for switch-based interceptions -- this means law enforcement will not be able to activate interceptions remotely or independently within the switching premises of a telecommunications carrier.").

approach to the review of carrier practices.

### B. Section 105 Of CALEA Was Not Intended To Involve The Commission In The Micromanagement Of Carrier Security Practices And Procedures

The industry comments confirm[15] -- and the FBI comments do not contradict -- that carriers' existing procedures provide a high level of security and confidentiality. As set forth in our comments, U S WEST has implemented call interceptions for years without incident.[16] Indeed, U S WEST's Security Department never has effectuated an unlawful interception; nor has our Court Order Processing Center ever compromised the confidentiality of a lawful interception. Other carriers report similar processes that are imbued with integrity and assure both the lawfulness of interceptions and the protection of subscriber's privacy. It is against this background of commendable carrier performance that Congress enacted Section 105 of CALEA and Section 229(b) of the Communications Act (which authorizes rules to implement Section 105).

Based on an apparent misunderstanding of the "system" concern incorporated into the statutory language and objectives of CALEA, the Notice proposes an enormously-detailed regulatory scheme to protect against risks that might be latent in current carrier practices and procedures. In fact, as demonstrated by the comments and the discussion above, far from seeking to protect against the conduct

---

[15] See, e.g., AirTouch Communications, Inc. ("AirTouch") at 19-20; BellSouth Corporation, et al. ("BellSouth") at 7-8; GTE Service Corporation ("GTE") at 6-7; SBC Communications Inc. ("SBC") at 12-14, 18; United States Telephone Association ("USTA") at 5-6.

[16] See U S WEST Comments at 16-17.

of carrier personnel, Section 105 was designed to ensure the continued involvement of carrier personnel in the process of implementing interceptions so that neither law enforcement entities nor unauthorized third parties would be able to use or abuse new computer technology to implement unauthorized interceptions.

With no Congressional or industry support for regulating carrier personnel procedures, and with no demonstrated public interest need, the Commission should reject the Notice's detailed mandates regarding carrier procedures. The comments demonstrate that there is simply no need for affidavits, employee designations, or recordkeeping rules.[17] As the comments make obvious, carriers are already carefully supervising the personnel that implement interceptions, and the Commission should not add another layer of bureaucratic requirements. Instead, the Commission should reorient its efforts towards the two real concerns that Congress had in mind when enacting Section 105, i.e., remote access to switches by law enforcement and/or hackers and the lack of carrier participation in the effectuation of process (to assure that only lawful effectuations occur).

### C. Regulations Directed At Carrier Procedures Should Be Far Less Intrusive Than The Measures Proposed In The Notice

As discussed in Part II.A and B. above, the Notice's proposed requirements with respect to carrier personnel are contrary to the purposes of Section 105. The Commission should, therefore, reject those requirements and rely instead on the successful security policies and procedures that carriers currently have in place.

[17] Compare id. at 22-30.

Moreover, the Commission should be extremely skeptical of the FBI's proposals regarding carrier procedures. The FBI apparently views CALEA as an all-purpose solution to law enforcement's needs (evidentiary and otherwise) regarding interceptions.[18] CALEA's scope, however, is limited to network capabilities and system security, and the statute gives the Commission no authority to become the regulator of interception procedures generally.

Below, U S WEST addresses certain of the specific proposals contained in the Notice and comments on the filings addressing the specific proposal. As we demonstrate, none of the Notice's proposals should be adopted.

1. Meaning Of "Appropriate Authorization" In Section 229(b)(1)

Section 229(b) directs the Commission to promulgate rules to implement Section 105 of CALEA. Under those rules, common carriers are required to establish appropriate policies and procedures to ensure "appropriate authorization to activate interception of communications or access to call-identifying information" and "to prevent any such interception or access without such authorization."[19] Carriers also must submit those policies and procedures to the Commission.[20]

As noted in our comments, U S WEST agrees with the Notice's tentative conclusion that the phrase "appropriate authorization" refers to the "authorization that a carrier's employee needs from the carrier to engage in interception activity."[21]

---

[18] See, e.g., FBI at 25 ¶ 55; id. at 29 ¶ 65.

[19] 47 U.S.C. § 229(b)(1) (emphasis added).

[20] See id. § 229(b)(3).

[21] U S WEST Comments at 18.

Other commentors make an argument that "appropriate authorization" may refer to the necessary external authorization from law enforcement.[22]

The statutory language may not permit a definitive resolution of this question.[23] What is important, however, is that neither interpretation of "appropriate authorization" gives the Commission authority to force carriers to conform their procedures to detailed regulatory mandates. There is no justification in the statute or sound policy for the Commission's rules specifying every detail of carrier compliance. Carrier policies to ensure "appropriate authorization" should at most be reviewed under a more flexible "safe harbor" or "guidelines" approach, with carrier certifications if necessary, as suggested in U S WEST's Comments.[24]

2. Substantive Rules On Lawful Interceptions

The Notice proposed a rule requiring carriers to define in their policies and procedures what legal authorizations are required to implement an interception.[25] In our comments, U S WEST opposed the Notice's tentative conclusion.[26] The FBI's

---

[22] See, e.g., 360° Communications Company ("360°") at 2-3; AT&T at 30-31; Ameritech Operating Companies ("Ameritech") at 3-4; CTIA at 27; SBC at 9-10.

[23] Those arguing for the latter interpretation might have a persuasive argument to the extent that a carrier is only required to determine external authorization from the face of the proffered process. See discussion immediately below at point 2.

[24] U S WEST Comments at 21-22. See, e.g., 360° at 5-7; BellSouth at 14-15; CTIA at 28; GTE at 10-11; Paging Network, Inc. ("PageNet") at 10-11; Personal Communications Industry Association ("PCIA") at 10-11; Sprint Spectrum L.P. d/b/a Sprint PCS ("Sprint") at 1 (all supporting self-certifications for all carriers).

[25] NPRM ¶ 29.

[26] See U S WEST Comments at 19-22.

comments indicate that law enforcement also doubts both the necessity and propriety of such a rule.[27]

As U S WEST pointed out in our comments, what constitutes a lawful interception is a matter of statutory mandate that the Commission cannot affect.[28] It is therefore unnecessary for the Commission to try to define or describe the legal bases for interceptions.

Furthermore, any such required list would unlawfully put carriers in the position of reviewing the merits of requested interceptions. In the words of the FBI, "carrier maintenance of such detailed authorization criteria could erroneously suggest to carrier personnel that they are entitled to substitute their review for that of a judge when a carrier is presented with a facially valid court order."[29]

The Commission should remember that carriers are implementers -- not authorizers -- of interceptions. The Commission should, therefore, not force carriers to inquire beyond the facial validity of either court orders or law enforcement certifications of exigent circumstances.

3. Designation Of Employees

The Notice proposed requiring carriers to designate certain employees who could implement interceptions and would be subject to greater security requirements.[30] In our comments, U S WEST urged the Commission to reject the

---

[27] See FBI at 22 ¶ 47.

[28] See U S WEST Comments at 20.

[29] See FBI at 22 ¶ 47.

[30] NPRM ¶¶ 30-33.

designated/non-designated distinction in its entirety and to rely instead on carriers' proven abilities and incentives to maintain the confidentiality of interceptions.[31] Other comments reveal general agreement among industry that the employee designation proposal both is unnecessary and exceeds the regulatory burden on carriers intended by Congress.[32]

As discussed in Part II.C.1 above, Section 229(b) requires rules to ensure that carriers "establish appropriate policies and procedures for the supervision and control" of officers and employees. The statute, in other words, gives the Commission a supervisory role but leaves it to carriers to establish specific policies and procedures. Imposing mandatory classifications on carrier employees exceeds that statutory mandate.

On the other hand, the FBI would have the Commission push the designated/non-designated distinction even further than proposed by the Notice. The FBI urges the Commission to establish special "vetting" procedures and reassignment policies for those carrier personnel designated to assist with interceptions.[33] U S WEST opposes such requirements because, as suggested above, they go well beyond the moderate regulatory role contemplated by the statute. Eliminating the Notice's employee designation proposal would prevent this overregulation, which merely duplicates the incentives carriers already have to

---

[31] See U S WEST Comments at 22-25.

[32] See, e.g., AirTouch at 24-25; AT&T at 32-33; BellSouth at 11, 13; GTE at 9; Powertel, Inc. ("Powertel") at 3-5; SBC at 19-20; USTA at 7. See also CDT at 15-16.

[33] See FBI at 19-20 ¶¶ 38-40.

maintain proper security and confidentiality.

The FBI also takes the unreasonable position that non-designated employees should not be involved in any task in which they could acquire "any knowledge, either express or implied" of an interception.[34] According to the FBI, "[e]ven the remote possibility that a non-designated employee might conclude that his work was in connection with a surveillance should be precluded."[35] As U S WEST stated in our comments, sensitive information associated with an interception is always maintained with strictest confidence by employees within U S WEST's Security Department.[36] Numerous other employees, however, will by necessity realize they are working on a Security Department project. There is no evidence to suggest that this minimal awareness by employees performing ministerial tasks has ever compromised the implementation of a lawful interception or individual expectations of privacy.

At a minimum, the Commission must reject the FBI's unworkable proposal regarding non-designated employees. At most, the Commission should institute a sort of guideline/practices review, perhaps accompanied by compliance affidavits.

4. Recordkeeping And Record Retention

The Notice proposed detailed recordkeeping and record retention requirements for carriers. The Notice suggested, for example, that carriers be required to create, within 48 hours of the start of each interception, detailed records

---

[34] See id. at 25 ¶ 56.

[35] Id. ¶ 57.

[36] See U S WEST Comments at 25-27.

of the interception.[37] In our comments, U S WEST opposed these requirements, arguing that our current recordkeeping policies are more than adequate for security and law enforcement purposes and that carriers should not have to restructure their recordkeeping procedures just to comply with a new regulatory mandate.[38] Comments submitted by other carriers reveal broad industry agreement that the Notice's proposals go too far and that a more flexible recordkeeping approach would be less costly and no less effective.[39]

Regarding record retention, the Notice suggested that carriers might be covered by the 10-year period specified in 18 U.S.C. Section 2518(8)(a).[40] However, as U S WEST and others noted in their comments, that statute applies only to law enforcement authorities.[41] The FBI also agreed and did not suggest any compelling reason why carriers should be under a significant record retention obligation.[42] Indeed, the policy justifications for the statutory 10-year retention period, such as preservation of evidence, are already accomplished by the requirement that law enforcement retain the records. As U S WEST stated in our comments, carriers should be allowed to determine for themselves -- based on industry custom, practice,

---

[37] NPRM ¶ 32.

[38] See U S WEST Comments at 29-31.

[39] See, e.g., AirTouch at 19, 21-24; AT&T at 34-35; BellSouth at 12-13; CTIA at 27; GTE 6-7; Nextel Communications, Inc. ("Nextel") at 15; SBC at 21-22; USTA at 6-8.

[40] NPRM ¶ 32.

[41] See U S WEST Comments at 30-31; AT&T at 35-36; Bell Atlantic Mobile, Inc. ("BAM") at 5-7; BellSouth Response to Regulatory Flexibility Analysis filed Dec. 12, 1997 at 3-4; USTA at 7-8.

[42] FBI at 30 ¶ 67 ("Law Enforcement understands that, while not necessarily required, carriers may wish to retain copies of those records.").

and standards -- how long to maintain their own interception records.[43]

### 5. Information Provided To Law Enforcement And The Commission

The Notice requested comment on whether carriers should be required to report all illegal wiretapping and compromises of the confidentiality of interceptions "to the Commission and/or the affected law enforcement agency or agencies."[44] In our comments, U S WEST opposed such a rule on the grounds that it was unnecessary and unwise.[45] Other carriers also criticized the proposed rule.[46]

In contrast, the FBI supported requiring carriers to report to the Commission "violations of [the carrier's] security policies and procedures and compromises, [or suspected compromises, of interceptions.]"[47] The FBI also proposed that carriers be required to report to law enforcement any compromise of an interception within two hours.[48]

As the carriers' comments make clear, the FBI's proposals are infirm from both a statutory and policy perspective. Thus, there is no legitimate basis for imposing reporting obligations on carriers in the circumstances addressed by the FBI.

The FBI does not suggest what statutory basis the Commission would have

---

[43] U S WEST Comments at 31.

[44] NPRM ¶ 27.

[45] See U S WEST Comments at 43-46.

[46] See, e.g., Ameritech at 5; SBC at 12-15.

[47] See FBI at 21-22 ¶ 45.

[48] See id. at 21 ¶ 43.

for promulgating the kinds of reporting rules it proposes. While the Commission has authority to promulgate rules to implement "the requirements of" CALEA,[49] the statute does not authorize the Commission to make general rules regarding interception procedures. Rather, CALEA mandates that carriers implement network capabilities and capacities and that they ensure systems security and integrity.

Moreover, there is no evidence that carriers have acted unlawfully or inappropriately with respect to occurrences of unlawful or compromised interceptions. To the extent a carrier believes that reporting the occurrence of an unlawful interception is appropriate, there already exist sufficient incentives to support reporting. Indeed, the record submissions indicated that some carriers engage in such reporting.[50] Any regulatory mandate that unlawful interceptions be reported to a non-law enforcement entity, such as the Commission, could conflict with a carrier's legal obligation and interest in maintaining the confidentiality of interceptions. As SBC pointed out, court orders authorizing interceptions typically prohibit carriers from disclosing the fact or content of an interception to any third party.[51] Informing the Commission of an unlawful interception would not only violate the court order but might subject a carrier to civil liability.

Similarly with compromised interceptions. While U S WEST has never been

---

[49] 47 U.S.C. § 229(a).

[50] See Ameritech at 5 (noting that it reports unlawful interceptions to law enforcement); SBC at 14.

[51] See SBC at 14.

involved in such an interception, it seems obvious that if any entity needs to be advised of such a compromise it is law enforcement -- not the Commission. Indeed, reporting the occurrence of a compromised interception outside of the law enforcement body directly involved in the interception activity would only increase the potential harm associated with the compromised interception itself.

Because there is no statutory basis for the Commission to require carriers to report unlawful or compromised interceptions and because there is no evidence that existing carrier practices thwart the objectives of CALEA, the Commission should refuse to adopt the FBI's proposal. The proposed carrier obligations are not required by statute and imposing them by regulatory fiat would be contrary to the public interest.

6. Implementation Of Interceptions

The FBI also urges that carriers should be required to implement emergency interceptions within two hours of receiving a request.[52] However, as discussed in Parts II.B and II.C.5 above, CALEA does not authorize the Commission to create general rules for interception procedures. Moreover, the FBI's proposal is needlessly rigid.

U S WEST and other carriers stand ready to assist law enforcement by effecting interceptions as expeditiously as possible, including accommodating emergency situations. In U S WEST's experience, two hours should be enough time to implement an emergency trap or trace-type of interception. The FBI's proposed

[52] See FBI at 31 ¶ 70.

two-hour rule -- applicable to all types of emergency interceptions -- is, however, too uncompromising. It makes no allowance for the varied types of emergency interceptions that might be involved or the specific circumstances under which carriers will have to effect the specific interception.

Because there is no statutory basis for the Commission to require carriers to effectuate emergency interceptions within two hours, nor any substantial evidence that carriers currently fail to respond appropriately to situations involving emergency interceptions, the Commission should refuse to adopt the FBI's proposal. The proposed carrier obligations are not required by statute and, like other of the FBI's proposals, imposing them by regulatory fiat would be contrary to the public interest.

## IV. THE INDUSTRY-DEVELOPED STANDARD MEETS THE REQUIREMENTS OF CALEA

The comments recognize that developing a standard to serve as a safe harbor for carriers is critical to the implementation of CALEA capability and capacity requirements.[53] In the absence of such a standard, compliance with CALEA would be far more costly and less efficient, and would result in the creation of numerous different solutions.

Industry now has adopted such a standard (J-STD-025). Under the statute, this standard constitutes a safe harbor, unless a party objects to the Commission and the Commission determines that the standard must be modified.

---

[53] See, e.g., AirTouch at 13-15; AT&T at 6-7; BellSouth at 15-16; USTA at 10. See also GTE at 11-14; Organization for the promotion and Advancement of Small Telecommunications Companies ("OPATSCO") at 5.

While the FBI asserts in its comments that the industry standard is "technologically deficient,"[54] it is obvious that this proceeding is not the appropriate forum to debate the sufficiency or deficiency of the standard.[55] Such should be addressed by the Commission only in the context of a petition by the FBI, or any other person objecting to the industry-adopted standard, pursuant to the procedure set forth in Section 107.

Accordingly, the Commission should be careful to avoid prejudging the merits of any of these issues in the context of this proceeding. For the time being, it is clear that, under the statute, the current industry standard is a safe harbor unless and until the Commission acts pursuant to an objection filed in accordance with Section 107.

---

[54] See FBI at 37 ¶ 88. The FBI's description in the "Background" section of its comments, which purports to be a straightforward narrative of various technological changes that allegedly motivated the adoption of CALEA (id. at 4 ¶ 6), are in reality descriptions of the very capabilities that are in dispute between industry and the FBI. For example, while the FBI expressed an interest in the ability to monitor independently the content of each "leg" of a multi-party conference call, industry believes that such a capability is not required by CALEA. Since the filing of the FBI comments, it appears that the FBI might be retreating from its prior position. Similarly, industry does not interpret CALEA to require the ability to identify who is part of a conference call at any time.

[55] Indeed, the Commission specifically placed this issue outside of the scope of the proceeding. NPRM ¶ 44.

## V. THE COMMENTS DEMONSTRATE THE NEED FOR A BLANKET TWO-YEAR EXTENSION OF THE COMPLIANCE DATE AND A DECLARATION THAT COMPLIANCE WILL NOT BE REASONABLY ACHIEVABLE UNTIL THE REQUISITE CAPABILITIES HAVE BEEN IMPLEMENTED IN EQUIPMENT COMMERCIALLY AVAILABLE ON AN INDUSTRYWIDE BASIS

The comments reveal a broad industry consensus that compliance with the capability requirements of CALEA is not reasonably achievable at this time and that compliance cannot be reasonably achievable until CALEA-compliant equipment is commercially available on an industrywide basis. U S WEST joins with those commentors that urge the Commission to grant a blanket two-year extension of the compliance date.[56] Furthermore, the Commission should make clear that further extensions will be given if compliant equipment is not commercially available at the time of the extended deadline.[57]

### A. The Record Demonstrates The Need For A Two-Year Extension Of The Compliance Date Under Section 107(c)

Overwhelming, commentors support the position that a key factor in evaluating whether compliance is "reasonably achievable" for purposes of granting an extension under Section 107(c) is whether the necessary technology has been

---

[56] See, e.g., 360° at 8; CTIA at 8; Motorola at 11; PageNet at 14-15; PrimeCo at 5-6; Telecommunications Industry Association ("TIA") at 10-11; United States Cellular Corporation ("USCC") at 3; USTA at 13-14. Such an extension is appropriate regardless of whether the Commission acts on CTIA's concomitant pending request that the Commission endorse the industry standard as a safe harbor standard.

[57] As U S WEST noted in our initial comments, and contrary to the suggestion in the comments of the Rural Telecommunications Group ("RTG") at 6-7, the Commission has the authority under Section 107(c) to grant "one or more" extensions of the compliance date. See U S WEST Comments at 37 n.65. Although the first such

implemented in telecommunications equipment available for purchase in the marketplace. It is undisputed that such equipment is not now available and will not be available at the time of the initial compliance date of October 1998. Accordingly, the Commission cannot sensibly defer dealing with this issue and is almost certain to face numerous petitions requesting extensions in the upcoming months if it does not grant an extension in the context of this proceeding.

Moreover, because an industry standard has only recently been developed and is still subject to criticism by the FBI and other law enforcement agencies, and because manufacturers will need time to develop and implement the technology necessary to meet this standard, compliance will not be reasonably achievable until at least October 2000. Thus, U S WEST joins other parties in urging the Commission to grant a blanket two-year extension.

### B. Compliance Is "Reasonably Achievable" Under Section 109(b) Only If The Necessary Technology Is Commercially Available On An Industrywide Basis

The Commission should also consider the commercial availability of CALEA-compliant technology in determining whether compliance is reasonably achievable for purposes of Section 109(b). If the requisite technology is not implemented in equipment commercially available to a carrier, then compliance clearly "would impose significant difficulty or expense on the carrier."[58] Moreover, considerations of competitive parity require that compliance not be deemed

---

extension may not reach beyond October 24, 2000, the Commission may grant further extensions after that date. And see OPATSCO at 8.

[58] 47 U.S.C. § 1008(b)(1).

reasonably achievable under Section 109(b) unless compliant equipment is available on an industrywide basis.

Furthermore, contrary to the FBI's suggestion that capacity requirements are irrelevant to capability deployment,[59] the FBI's delay in publishing the requisite capacity requirements does impact on the issue of capability features. The ultimate designation of capacity will affect the design and deployment of technology capable of providing the necessary capabilities. Thus, the development of final capacity requirements will inevitably affect when and if compliance with the capability requirements is reasonably achievable.[60]

U S WEST also urges the Commission to create a presumption that where compliance is not reasonably achievable with respect to particular equipment involving a particular carrier that compliance is not reasonably achievable with respect to that equipment for other carriers. Such a presumption is warranted by the fact that almost all the statutory factors the Commission must consider under Section 109(b) will not vary between carriers.[61] Moreover, such a presumption will

---

[59] See FBI at 39 ¶ 92.

[60] U S WEST agrees with AT&T and CTIA, that -- in order to ensure that industry has a fair opportunity to respond to positions such as those taken by the FBI in this proceeding regarding the meaning and operation of CALEA provisions -- the Commission must ensure that the FBI's participation in Section 109(b) proceedings is entirely on the record. AT&T at 21; CTIA at 22-23 (regarding Section 109(b) proceedings and arguing that a similar policy of openness should be accorded in Section 107 proceedings, even though that provision requires consultation with the FBI).

[61] Those criteria include, inter alia, "the effect on public safety and national security; the effect on rates for basic residential telephone service; the effect on the nature and cost of the equipment, facility, or service at issue; the effect on the operation of